

# IRS News Release

---

Media Relations Office

Washington, D.C.

Media Contact: 202.622.4000

[www.irs.gov/newsroom](http://www.irs.gov/newsroom)

Public Contact: 800.829.1040

---

## **IRS Urges Caution about Internet Sites that Resemble the Official IRS Site**

IR-2007-58, March 13, 2007

WASHINGTON — The Internal Revenue Service today reminded taxpayers that the address of the official IRS government Web site is [www.irs.gov](http://www.irs.gov).

Taxpayers may be confused by the proliferation of Internet sites that contain some form of the Internal Revenue Service name or IRS acronym with a .com, .net, .org or other designation in the address instead of .gov. Since many of these sites also bear a striking resemblance to the real IRS site, taxpayers may be misled into thinking that the site they have accessed is indeed the official IRS government site. These sites are not the official IRS Web site and have no connection to the official IRS site or to the IRS.

“There is one legitimate IRS site: IRS.gov,” said IRS Commissioner Mark W. Everson. “Always check carefully and make sure you know what Web site you are using.”

Because .com, .net and .org are such common parts of Internet addresses, taxpayers may automatically or inadvertently type these extensions, instead of .gov, into the address line of their Web browser when trying to find the genuine IRS Web site.

Following recent concerns that Internet sites may be causing confusion among taxpayers, the IRS is working with the Treasury Inspector General for Tax Administration on this matter. TIGTA has authority to review issues protecting the integrity of tax administration, including impersonation of the IRS. The IRS and TIGTA are committed to ensuring that taxpayers are not misled.

Although the IRS Web site offers interactive features, the tax or private financial information that these features ask the taxpayer for is extremely limited. The IRS reminds consumers who access unfamiliar sites, or sites they have never dealt with before, that they should never reveal any personal or financial information, such as credit, bank account or PIN numbers, without verifying the validity of the site.

The IRS also reminds consumers to be alert to an on-going Internet scam in which consumers receive an e-mail informing them of a federal tax refund. The e-mail, which claims to be from the IRS, directs the consumer to a link — often a Web site resembling the IRS Web site — that requests personal and financial information, such as Social Security number and credit card information.

—More—

This scheme is an attempt to trick the e-mail recipients into disclosing their personal and financial data. The practice is called “phishing” for information.

The information fraudulently obtained is then used to steal the taxpayer’s identity and financial assets. Generally, identity thieves use someone’s personal data to steal his or her financial accounts, run up charges on the victim’s existing credit cards, apply for new loans, credit cards, services or benefits in the victim’s name and even file fraudulent tax returns.

Taxpayers who receive an unsolicited e-mail purporting to be from the IRS should never click on any links in the message, open any attachments or provide any personal or financial information to the sender.